Додаток 1

**Технічні характеристики:**

|  |  |
| --- | --- |
| Модель | Алмаз-1К |
| Формфактор | Малогабаритний знімний USB-пристрій |
| Протокол обміну | CCID-інтерфейс |
| Інтерфейс підключення | USB 2.0 або 3.0 |
| Технологічні особливості | Виготовлений на двошаровій друкованій платі, яка залита компаундом, що формує захисний шар, та встановлена в пластмасовий корпус. На друкованій платі встановлюються електроні компоненти та USB-з’єднувач типу А-plug (виделка) |
| Криптографічні алгоритми та протоколи | - шифрування за ДСТУ ГОСТ 28147:2009 (режим простої заміни та режим вироблення імітовставки);  - ЕЦП за ДСТУ 4145-2002 (всі довжини ключів передбачені стандартом);  - гешування за ГОСТ 34.311-95;  - протокол розподілу ключових даних Діффі-Гелмана в групі точок еліптичної кривої (довжина ключа до 571 біту) |
| Швидкість формування ЕЦП за ДСТУ 4145-2002, поле 257 | 500 мс |
| Швидкість формування спільного секрету Діффі-Гелмана в гр.т. еліптичної кривої, поле 571 | 2100 мс |
| Експертний висновок Державної служби спеціального зв'язку та захисту інформації України | Так |
| Операційні системи, які підтримуються | Microsoft Windows (32/64-біт) 7, 2003 Server, 8, 10, 2012 Server, 2016 Server |
| Кількість гарантованих робочих циклів під’єднань-від’єднань пристрою (до виходу з ладу) | не менше 5 000 |
| Термін зберігання даних у пам’яті | не менше 10 років |
| Інші особливості | - Інтерфейси засобів криптографічного захисту інформації, що реалізовані в пристрої, відповідають вимогам наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв’язку та захисту інформації України від 27.12.2013 № 2782/5/689 «Про затвердження вимог до алгоритмів, форматів та інтерфейсів, що реалізуються у засобах шифрування та надійних засобах електронного цифрового підпису», зареєстрованого в Міністерстві юстиції України 27.12.2013 за № 2228/24759 (повинно бути підтверджено чинним експертним висновком в галузі криптографічного захисту інформації)  - Ключі генеруються, зберігаються та використовуються тільки усередині електронного ключа, та жодним способом не потрапляють за його межі.  - Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому постійному запам’ятовуючому пристрої електронного ключа.  - На корпусі кожного пристрою нанесений індивідуальний серійний чи заводський номер.  - Пристрій має можливість ведення та перегляду журналу реєстрації подій (фіксуються події, які пов’язані із генерацією ключів, зміною паролю, спробами ввести невірний пароль доступу тощо). |
| Гарантія | не менше 36 місяців |